FIG. 1

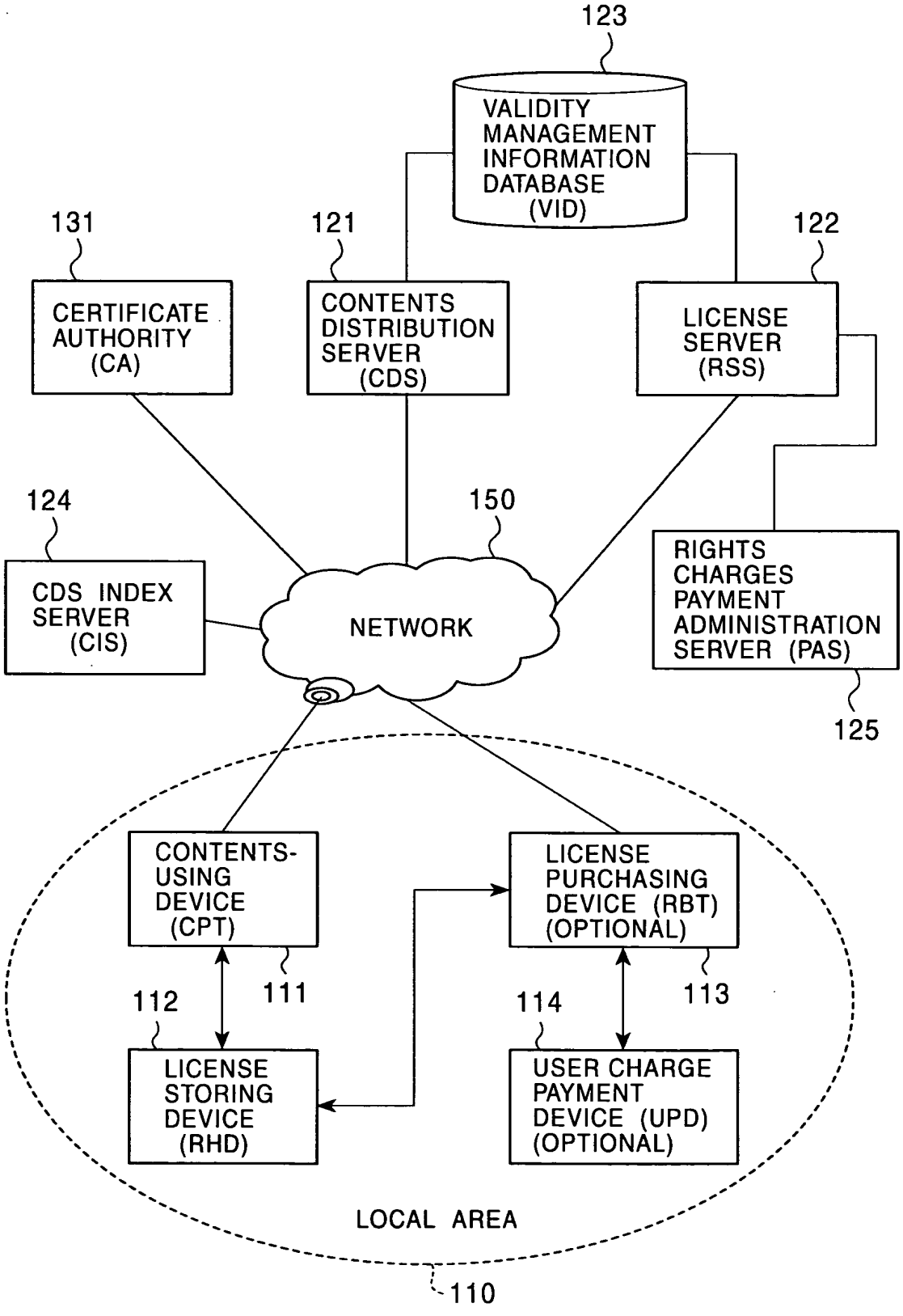

123
VALIDITY MANAGEMENT INFORMATION DATABASE (VID)
131
CERTIFICATE AUTHORITY (CA)
121
CONTENTS DISTRIBUTION SERVER (CDS)
122
LICENSE SERVER (RSS)
124
CDS INDEX SERVER (CIS)
150
NETWORK
RIGHTS CHARGES PAYMENT ADMINISTRATION SERVER (PAS)
125
CONTENTS-USING DEVICE (CPT)
LICENSE PURCHASING DEVICE (RBT) (OPTIONAL)
112
111
114
113
LICENSE STORING DEVICE (RHD)
USER CHARGE PAYMENT DEVICE (UPD) (OPTIONAL)
LOCAL AREA
110

FIG. 2

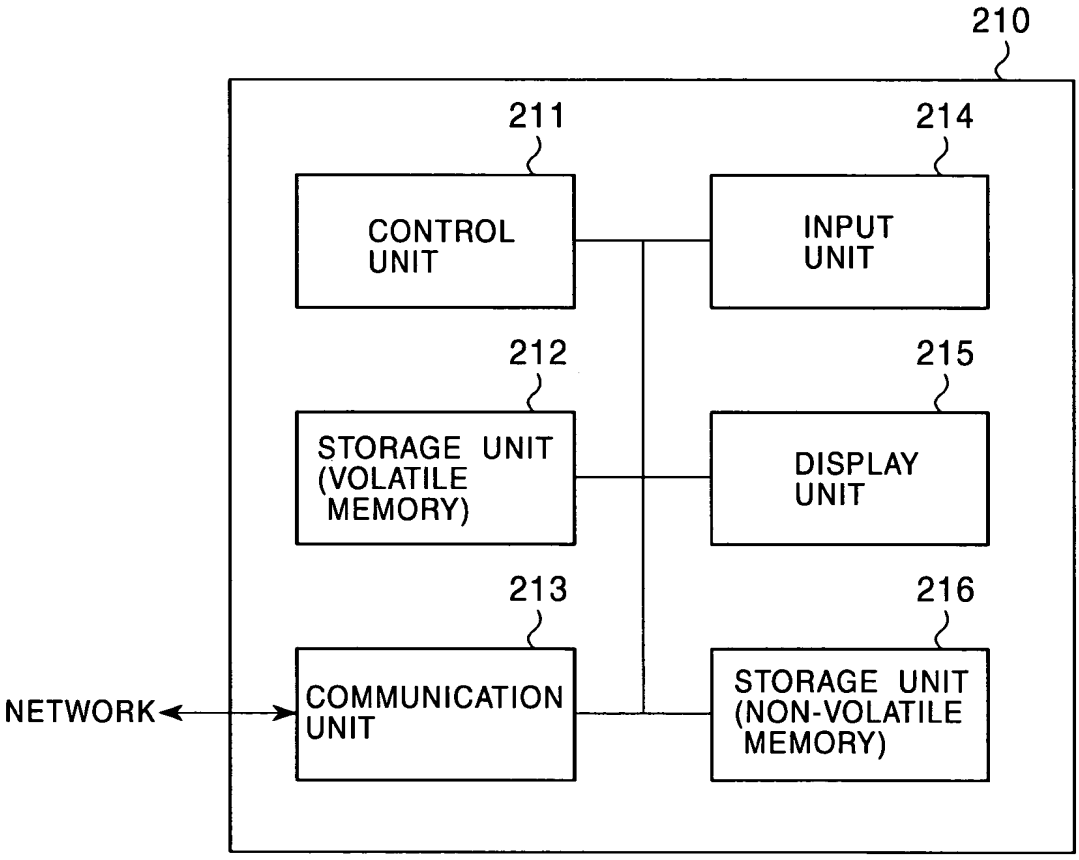

210
211
214
CONTROL UNIT
INPUT UNIT
212
215
STORAGE UNIT (VOLATILE MEMORY)
DISPLAY UNIT
213
216
NETWORK
COMMUNICATION UNIT
STORAGE UNIT (NON-VOLATILE MEMORY)

FIG. 3

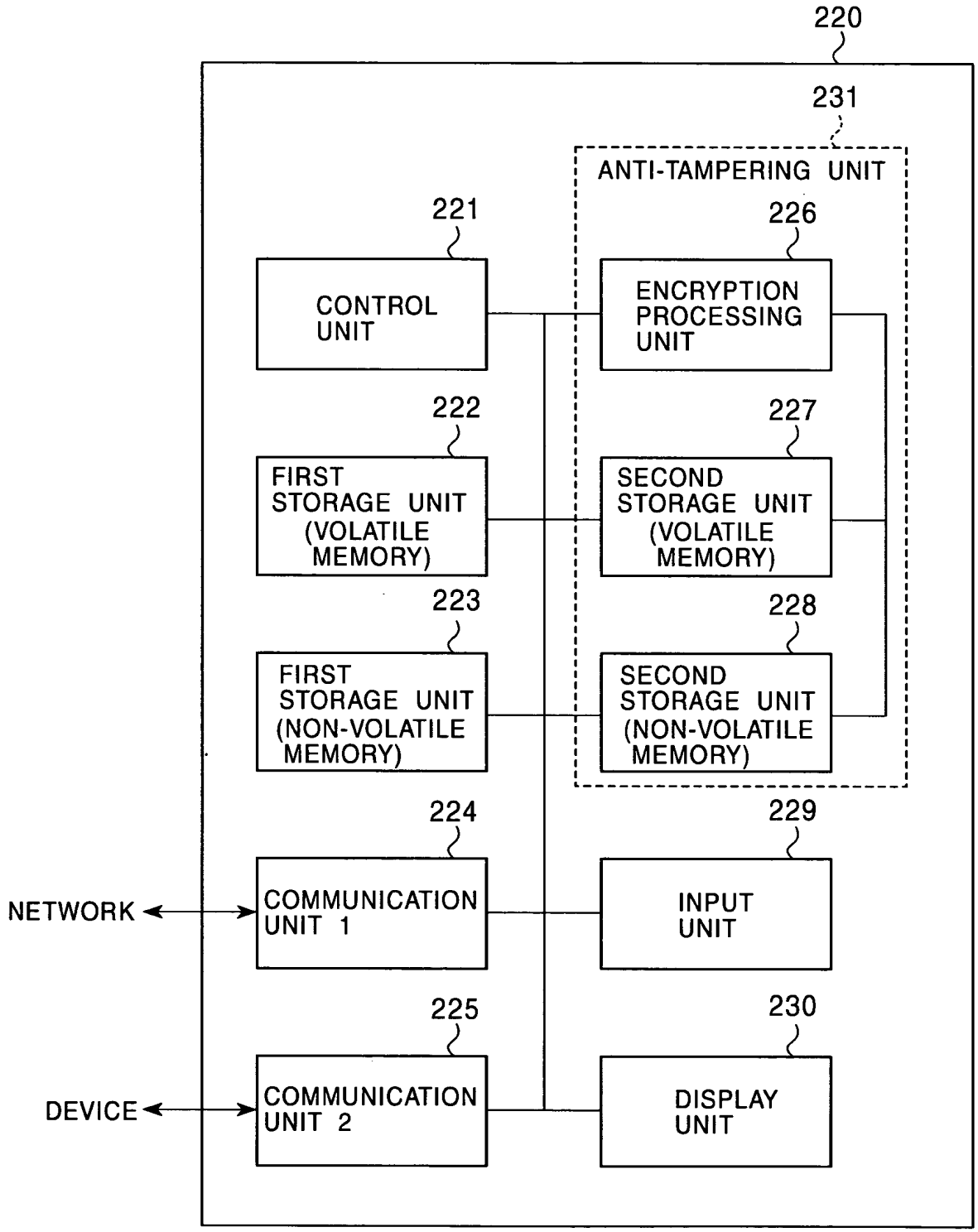

220
231
ANTI-TAMPERING UNIT
221
CONTROL UNIT
226
ENCRYPTION PROCESSING UNIT
222
FIRST STORAGE UNIT (VOLATILE MEMORY)
227
SECOND STORAGE UNIT (VOLATILE MEMORY)
223
FIRST STORAGE UNIT (NON-VOLATILE MEMORY)
228
SECOND STORAGE UNIT (NON-VOLATILE MEMORY)
224
COMMUNICATION UNIT 1
229
INPUT UNIT
NETWORK
225
COMMUNICATION UNIT 2
230
DISPLAY UNIT
DEVICE

FIG. 4

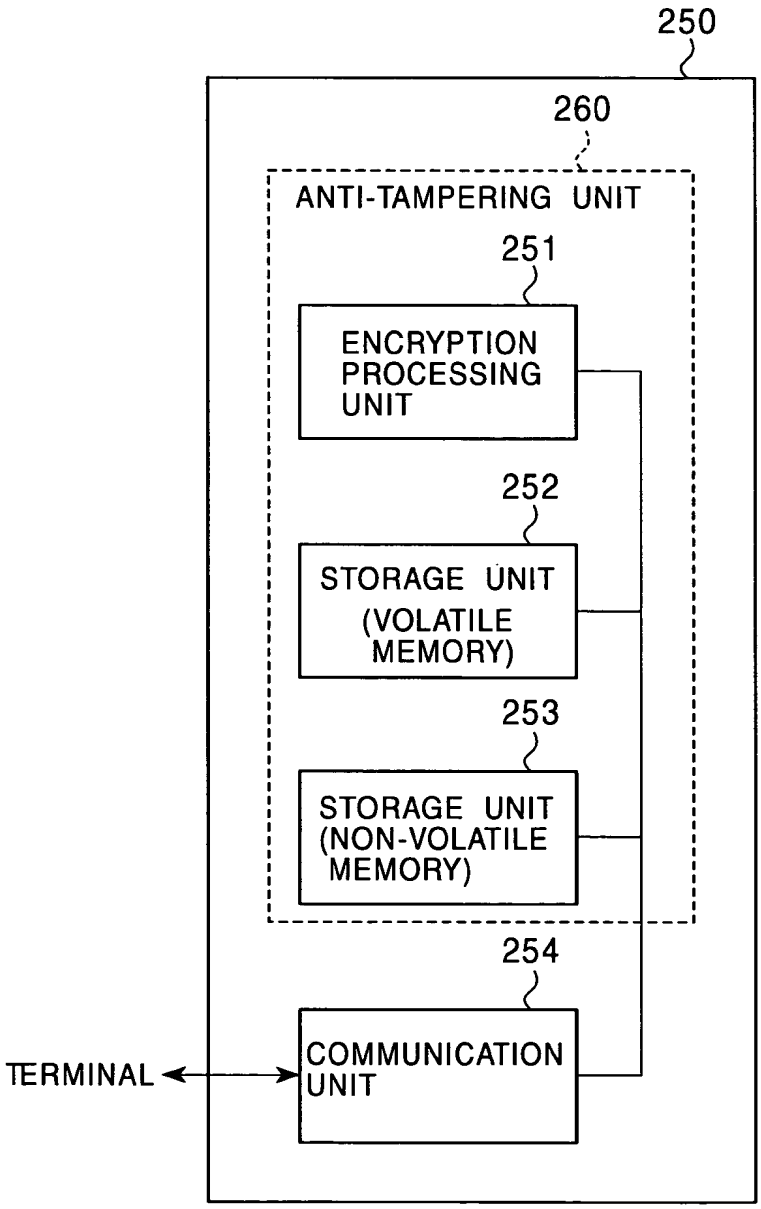

250
260
ANTI-TAMPERING UNIT
251
ENCRYPTION PROCESSING UNIT
252
STORAGE UNIT (VOLATILE MEMORY)
253
STORAGE UNIT (NON-VOLATILE MEMORY)
254
COMMUNICATION UNIT
TERMINAL

FIG. 5A

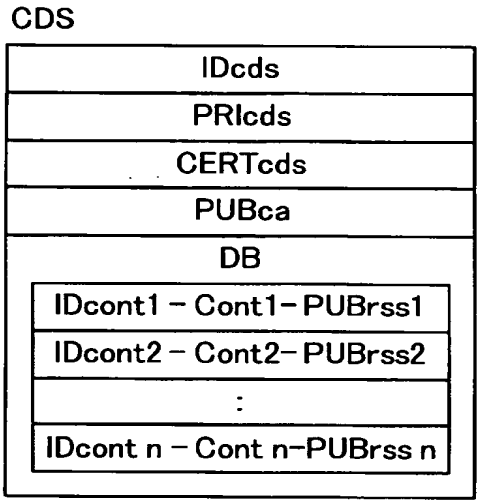


FIG. 5B

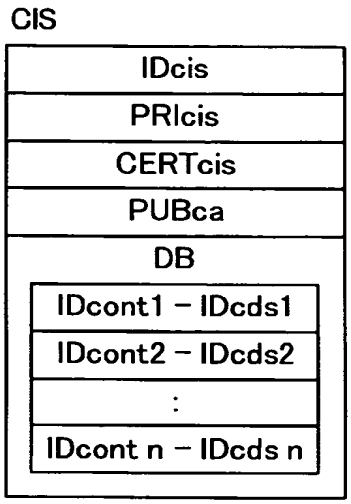


FIG. 5C

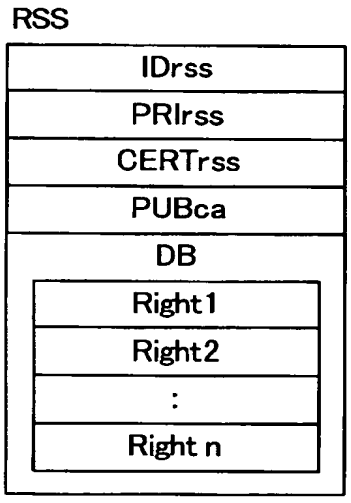


FIG. 5D

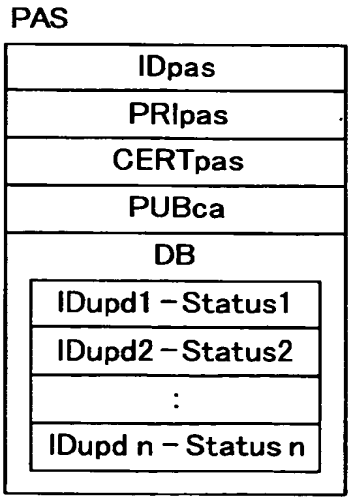


FIG. 6A

(IN ANTI-TAMPERING UNIT: (e)CPT)

IDcpt	PRIcpt	CERTcpt	PUBca	IDcis	Ksto1	Ksto2

FIG. 6B

(OUT OF ANTI-TAMPERING UNIT: (f)CPT)

DB
Cont1+MAC
Cont2+MAC
:
Cont n+MAC

FIG. 6C

(g)RHD

IDrhd	PRIrhd	CERTrhd	PUBca	DB

DB:

Right1
Right2
:
Right n

FIG. 6D

(IN ANTI-TAMPERING UNIT: (h)RBT)

IDrbt	PRIrbt	CERTrbt	PUBca

FIG. 6E

(i)UPD

IDupd	PRIupd	CERTupd	PUBca

FIG. 7

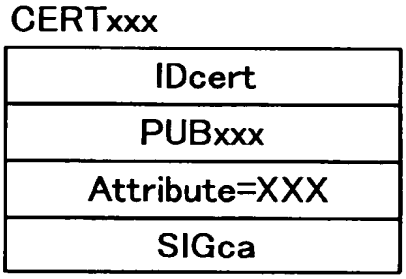


FIG. 8

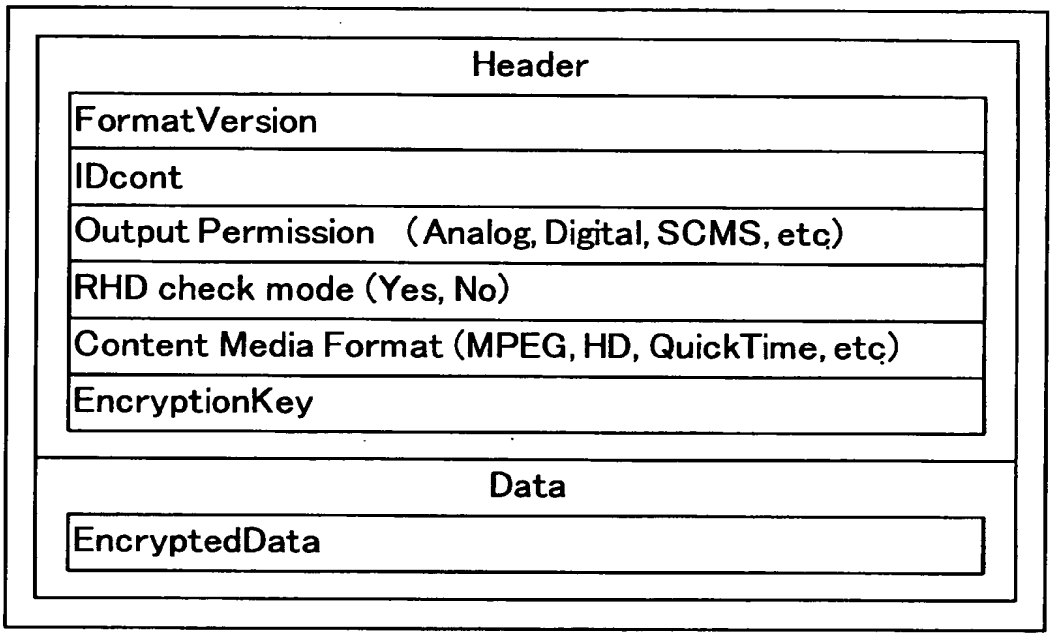

Header
FormatVersion
IDcont
Output Permission (Analog, Digital, SCMS, etc)
RHD check mode (Yes, No)
Content Media Format (MPEG, HD, QuickTime, etc)
EncryptionKey
Data
EncryptedData

FIG. 9

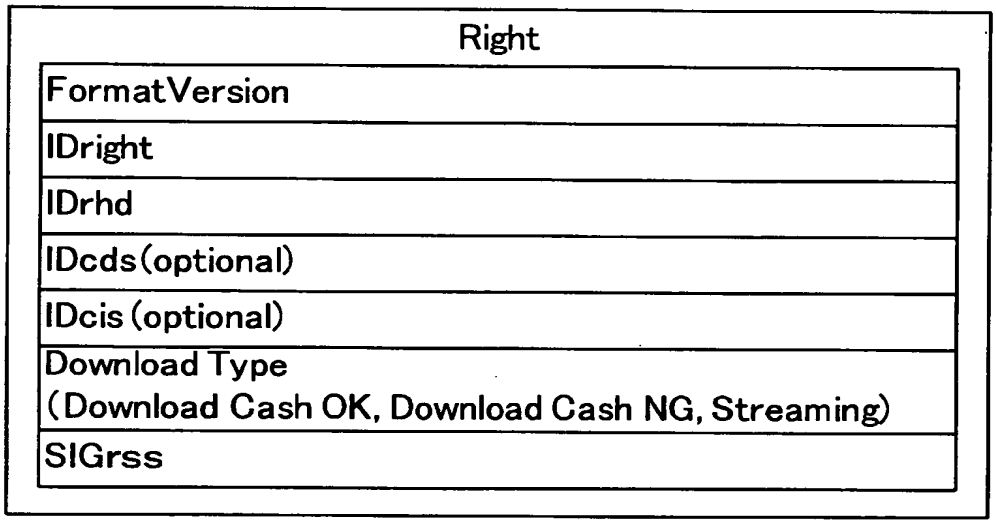

Right
FormatVersion
IDright
IDrhd
IDcds(optional)
IDcis (optional)
Download Type
(Download Cash OK, Download Cash NG, Streaming)
SIGrss

FIG. 10A

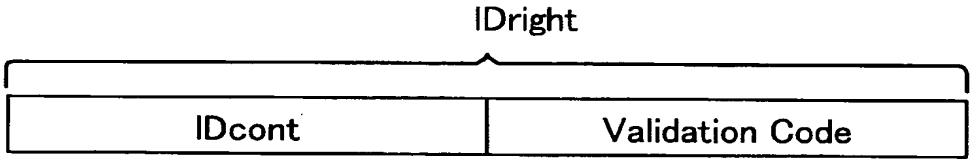


FIG. 10B

IDcont	Validation Code	Start	End	REMAINING COUNT
IDcont1	VC1	2002/02/25, 0:00	2002/02/03, 0:00	—
	VC2	2002/04/01, 0:00	—	—
IDcont2	VC1	—	2099/12/31, 23:59	—
	VC2	—	—	10
	VC3	—	—	10
IDcont3	VC1	—	—	20
	VC2	—	—	99
:	:	:	:	:
IDcont n	VCm	—	2099/12/31, 23:59	50

FIG. 11

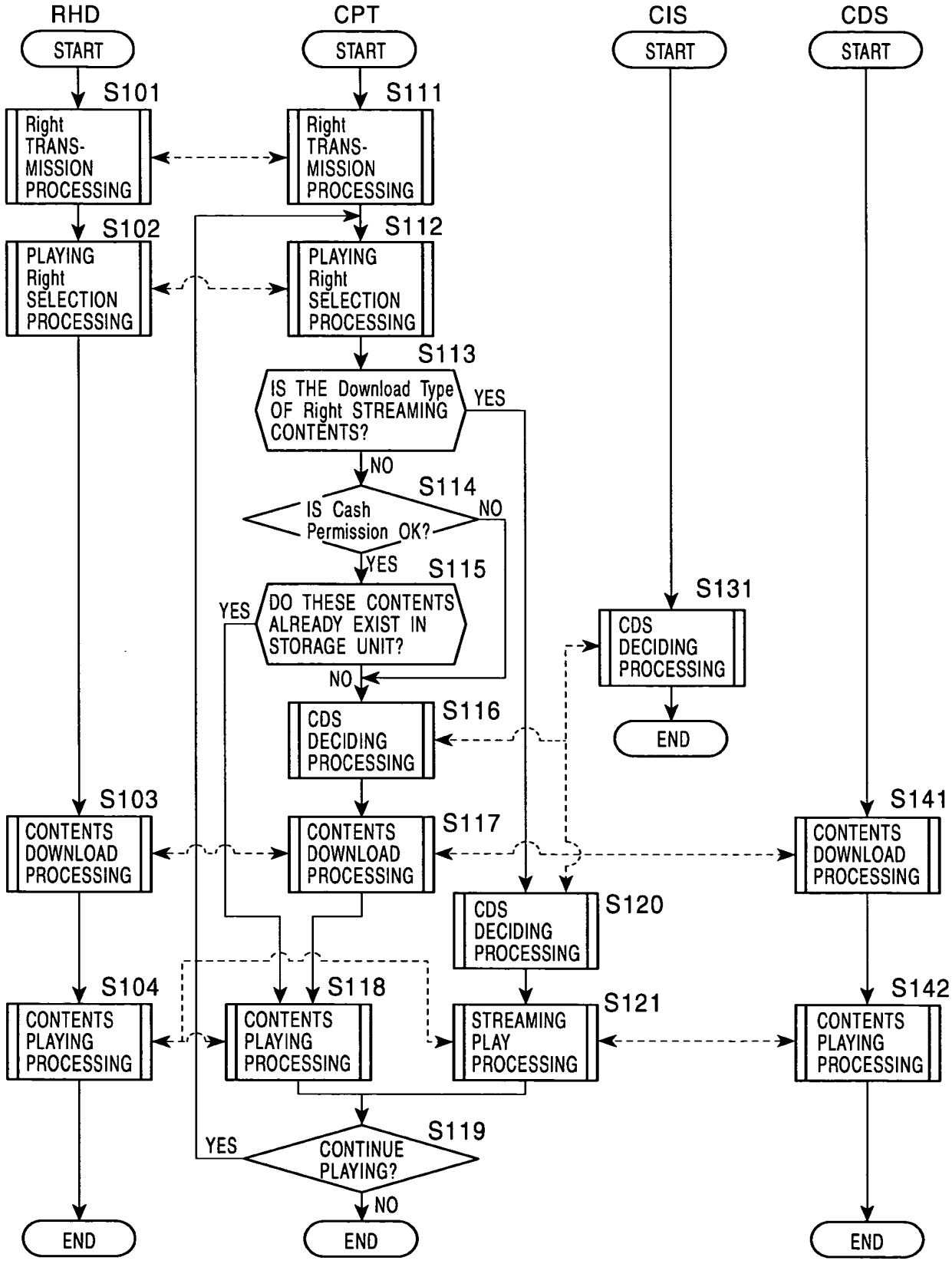

RHD
CPT
CIS
CDS
START
START
START
START
S101
Right TRANS-MISSION PROCESSING
S111
Right TRANS-MISSION PROCESSING
S102
PLAYING Right SELECTION PROCESSING
S112
PLAYING Right SELECTION PROCESSING
S113
IS THE Download Type OF Right STREAMING CONTENTS?
YES
NO
S114
IS Cash Permission OK?
NO
YES
S115
DO THESE CONTENTS ALREADY EXIST IN STORAGE UNIT?
YES
NO
S131
CDS DECIDING PROCESSING
END
S116
CDS DECIDING PROCESSING
S103
CONTENTS DOWNLOAD PROCESSING
S117
CONTENTS DOWNLOAD PROCESSING
S141
CONTENTS DOWNLOAD PROCESSING
S120
CDS DECIDING PROCESSING
S104
CONTENTS PLAYING PROCESSING
S118
CONTENTS PLAYING PROCESSING
S121
STREAMING PLAY PROCESSING
S142
CONTENTS PLAYING PROCESSING
S119
YES
CONTINUE PLAYING?
NO
END
END
END

FIG. 12

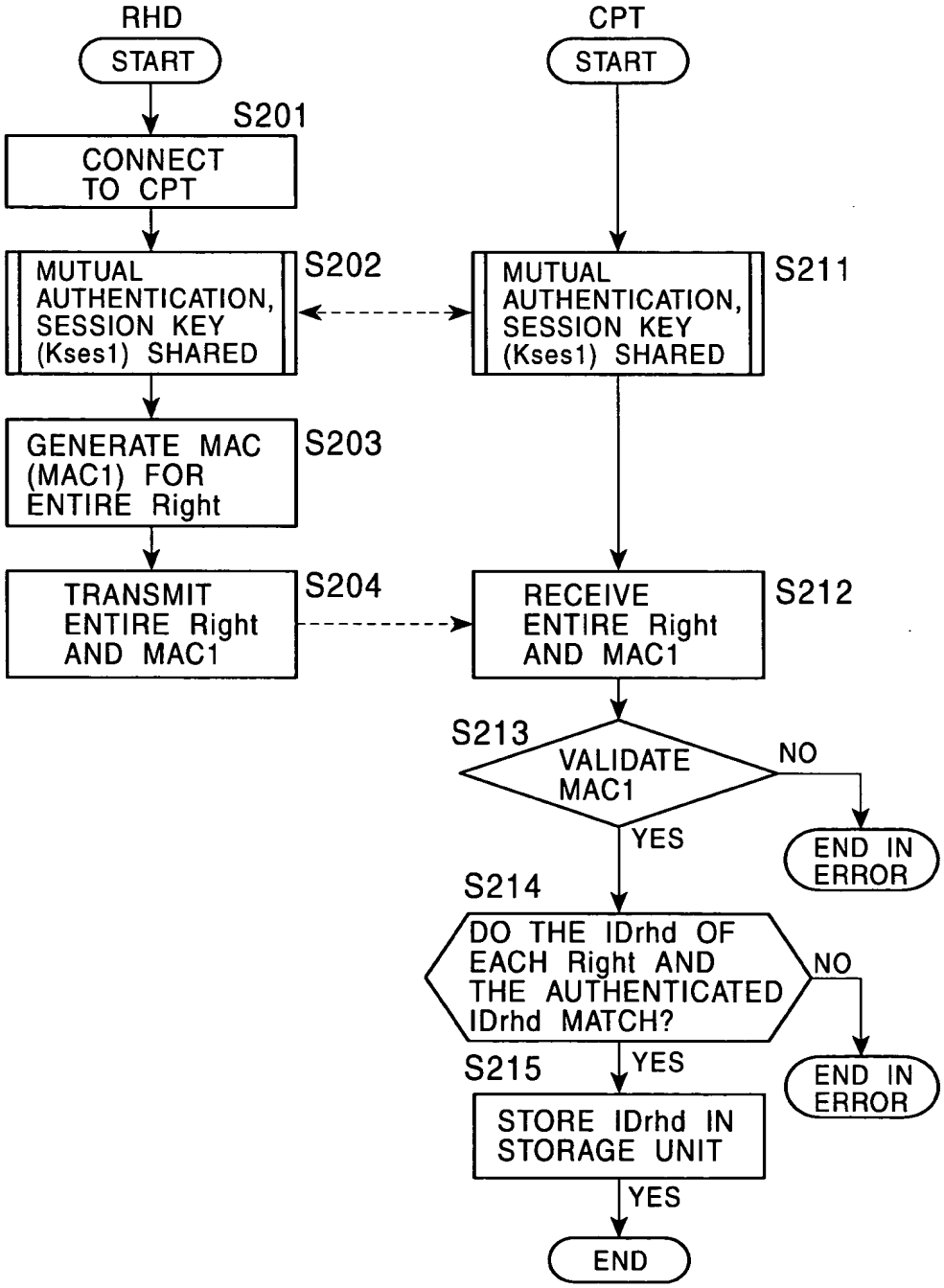

RHD
START
S201
CONNECT TO CPT
MUTUAL AUTHENTICATION, SESSION KEY (Kses1) SHARED
S202
GENERATE MAC (MAC1) FOR ENTIRE Right
S203
TRANSMIT ENTIRE Right AND MAC1
S204
CPT
START
MUTUAL AUTHENTICATION, SESSION KEY (Kses1) SHARED
S211
RECEIVE ENTIRE Right AND MAC1
S212
S213
VALIDATE MAC1
NO
YES
END IN ERROR
S214
DO THE IDrhd OF EACH Right AND THE AUTHENTICATED IDrhd MATCH?
NO
YES
END IN ERROR
S215
STORE IDrhd IN STORAGE UNIT
YES
END

FIG. 13

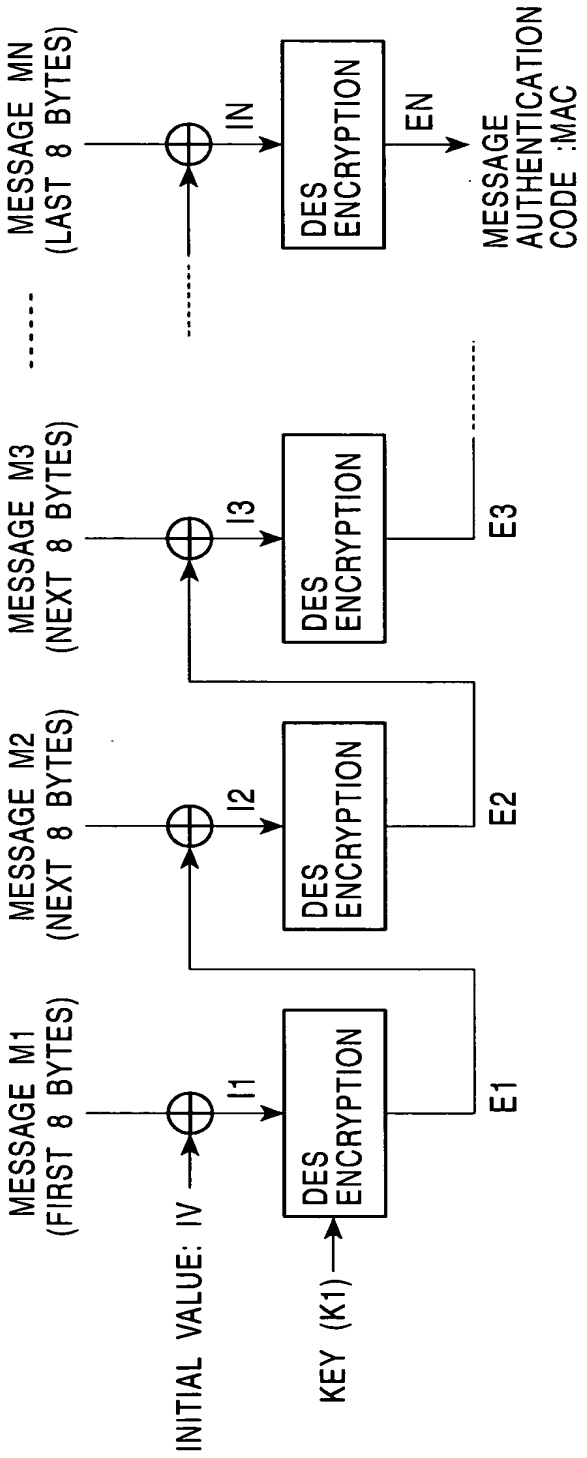

MESSAGE M1
(FIRST 8 BYTES)
MESSAGE M2
(NEXT 8 BYTES)
MESSAGE M3
(NEXT 8 BYTES)
MESSAGE MN
(LAST 8 BYTES)
INITIAL VALUE: IV
KEY (K1)
I1
I2
I3
IN
DES ENCRYPTION
E1
E2
E3
EN
MESSAGE AUTHENTICATION CODE :MAC
:EXCLUSIVE-OR PROCESSING (INCREMENTS OF 8 BYTES)

FIG. 14

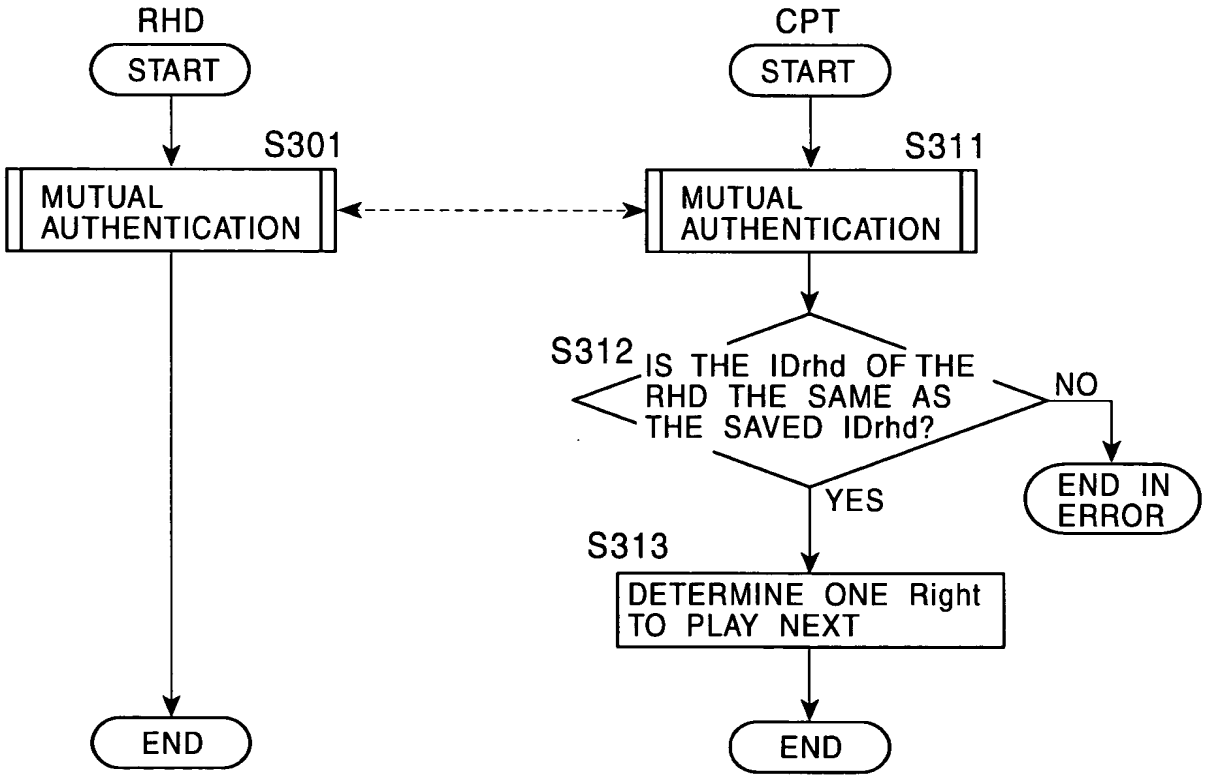

RHD
START
S301
MUTUAL AUTHENTICATION
END
CPT
START
S311
MUTUAL AUTHENTICATION
S312
IS THE IDrhd OF THE RHD THE SAME AS THE SAVED IDrhd?
NO
END IN ERROR
YES
S313
DETERMINE ONE Right TO PLAY NEXT
END

FIG. 15

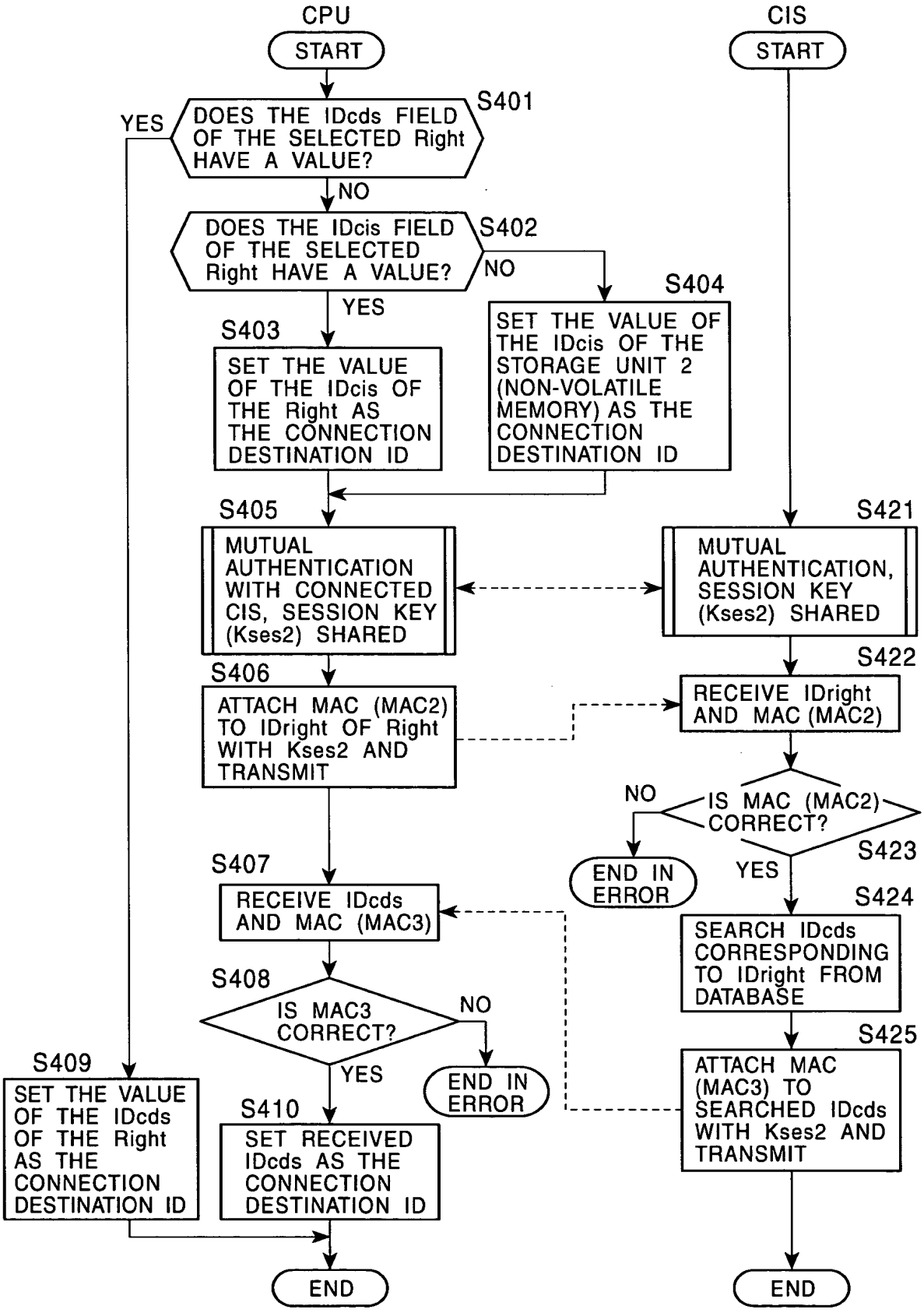

CPU
START
S401
DOES THE IDcds FIELD OF THE SELECTED Right HAVE A VALUE?
YES
NO
S402
DOES THE IDcis FIELD OF THE SELECTED Right HAVE A VALUE?
NO
YES
S403
SET THE VALUE OF THE IDcis OF THE Right AS THE CONNECTION DESTINATION ID
S404
SET THE VALUE OF THE IDcis OF THE STORAGE UNIT 2 (NON-VOLATILE MEMORY) AS THE CONNECTION DESTINATION ID
S405
MUTUAL AUTHENTICATION WITH CONNECTED CIS, SESSION KEY (Kses2) SHARED
S406
ATTACH MAC (MAC2) TO IDright OF Right WITH Kses2 AND TRANSMIT
S407
RECEIVE IDcds AND MAC (MAC3)
S408
IS MAC3 CORRECT?
NO
YES
END IN ERROR
S409
SET THE VALUE OF THE IDcds OF THE Right AS THE CONNECTION DESTINATION ID
S410
SET RECEIVED IDcds AS THE CONNECTION DESTINATION ID
END
CIS
START
S421
MUTUAL AUTHENTICATION, SESSION KEY (Kses2) SHARED
S422
RECEIVE IDright AND MAC (MAC2)
NO
IS MAC (MAC2) CORRECT?
S423
YES
END IN ERROR
S424
SEARCH IDcds CORRESPONDING TO IDright FROM DATABASE
S425
ATTACH MAC (MAC3) TO SEARCHED IDcds WITH Kses2 AND TRANSMIT
END

FIG. 16

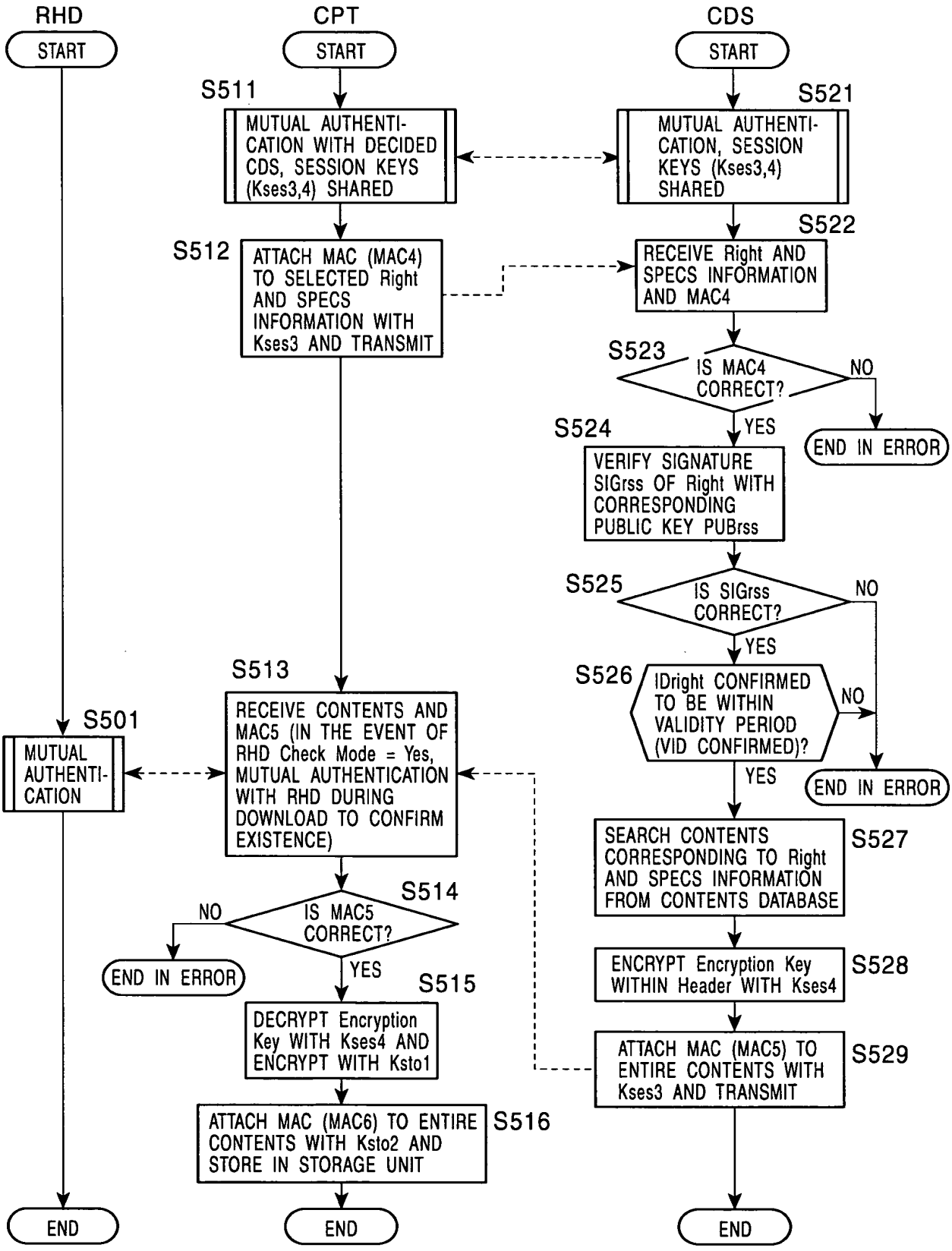

RHD
START
CPT
START
CDS
START
S511
MUTUAL AUTHENTI-CATION WITH DECIDED CDS, SESSION KEYS (Kses3,4) SHARED
S521
MUTUAL AUTHENTI-CATION, SESSION KEYS (Kses3,4) SHARED
S512
ATTACH MAC (MAC4) TO SELECTED Right AND SPECS INFORMATION WITH Kses3 AND TRANSMIT
S522
RECEIVE Right AND SPECS INFORMATION AND MAC4
S523
IS MAC4 CORRECT?
NO
YES
END IN ERROR
S524
VERIFY SIGNATURE SIGrss OF Right WITH CORRESPONDING PUBLIC KEY PUBrss
S525
IS SIGrss CORRECT?
NO
YES
S526
IDright CONFIRMED TO BE WITHIN VALIDITY PERIOD (VID CONFIRMED)?
NO
YES
END IN ERROR
S501
MUTUAL AUTHENTI-CATION
S513
RECEIVE CONTENTS AND MAC5 (IN THE EVENT OF RHD Check Mode = Yes, MUTUAL AUTHENTICATION WITH RHD DURING DOWNLOAD TO CONFIRM EXISTENCE)
S514
IS MAC5 CORRECT?
NO
YES
END IN ERROR
S515
DECRYPT Encryption Key WITH Kses4 AND ENCRYPT WITH Ksto1
S516
ATTACH MAC (MAC6) TO ENTIRE CONTENTS WITH Ksto2 AND STORE IN STORAGE UNIT
S527
SEARCH CONTENTS CORRESPONDING TO Right AND SPECS INFORMATION FROM CONTENTS DATABASE
S528
ENCRYPT Encryption Key WITHIN Header WITH Kses4
S529
ATTACH MAC (MAC5) TO ENTIRE CONTENTS WITH Kses3 AND TRANSMIT
END
END
END

FIG. 17

FORMAT

AUDIO PLAYBACK CAPABILITIES	IMAGE PLAYBACK CAPABILITIES	COMMUNICATION PATH

FORMAT

5.1ch	NTSC	100Mbps

FORMAT

Stereo	100 x 200 DOT MONITOR	64Kbps

FIG. 18

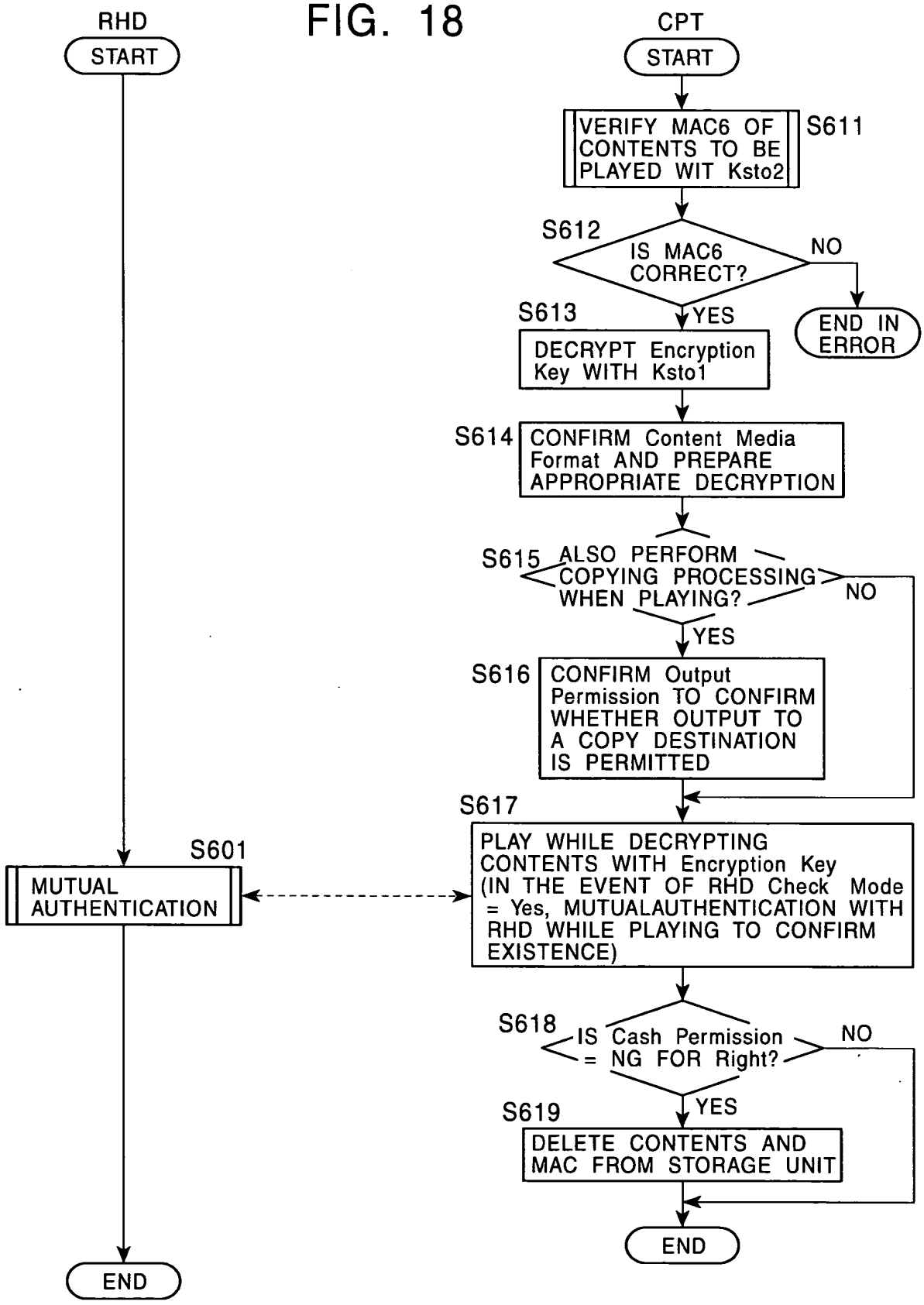

RHD
START
S601
MUTUAL AUTHENTICATION
END
CPT
START
VERIFY MAC6 OF CONTENTS TO BE PLAYED WIT Ksto2
S611
S612
IS MAC6 CORRECT?
NO
END IN ERROR
YES
S613
DECRYPT Encryption Key WITH Ksto1
S614
CONFIRM Content Media Format AND PREPARE APPROPRIATE DECRYPTION
S615
ALSO PERFORM COPYING PROCESSING WHEN PLAYING?
NO
YES
S616
CONFIRM Output Permission TO CONFIRM WHETHER OUTPUT TO A COPY DESTINATION IS PERMITTED
S617
PLAY WHILE DECRYPTING CONTENTS WITH Encryption Key (IN THE EVENT OF RHD Check Mode = Yes, MUTUALAUTHENTICATION WITH RHD WHILE PLAYING TO CONFIRM EXISTENCE)
S618
IS Cash Permission = NG FOR Right?
NO
YES
S619
DELETE CONTENTS AND MAC FROM STORAGE UNIT
END

FIG. 19

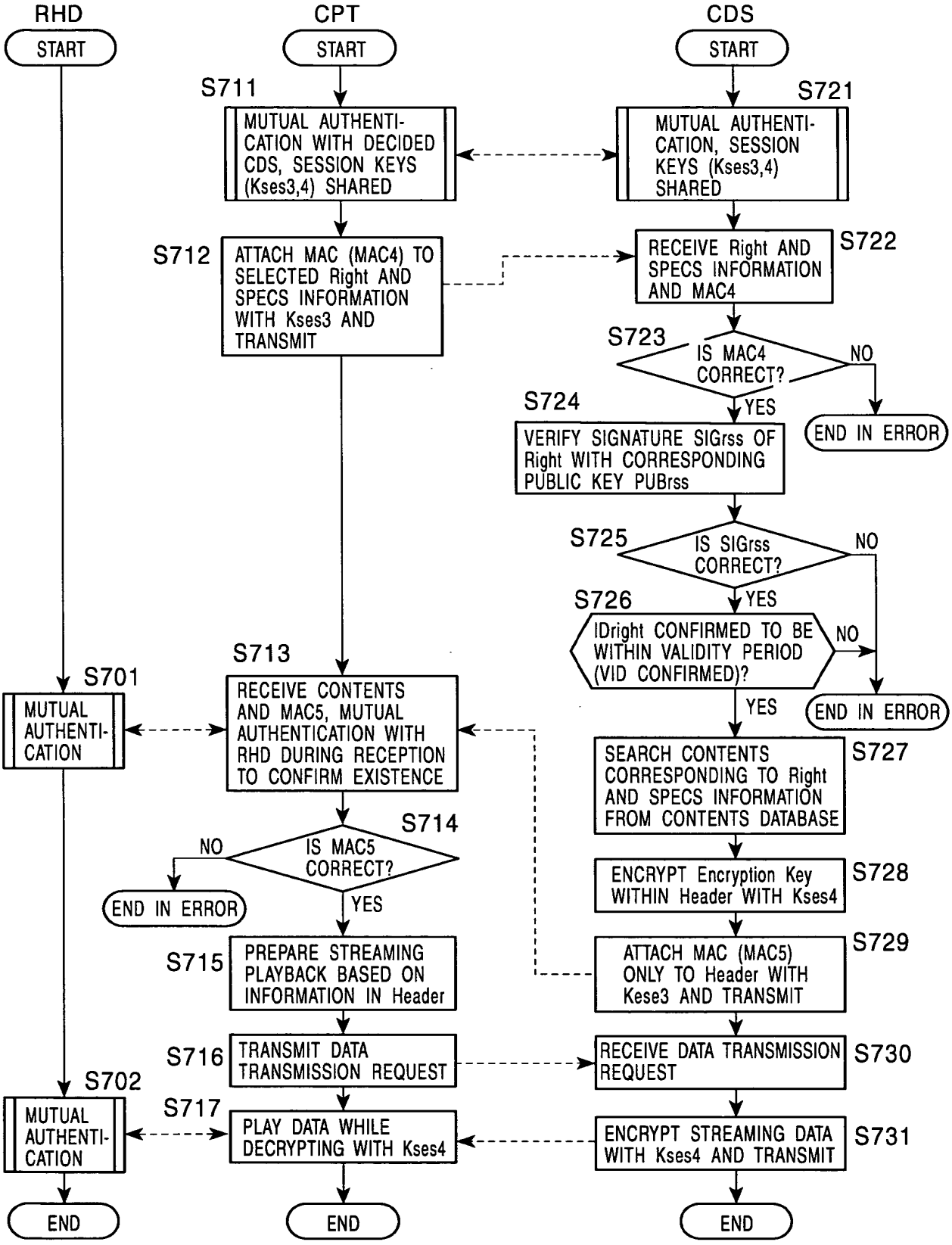

RHD
CPT
CDS
START
START
START
S711
MUTUAL AUTHENTI-CATION WITH DECIDED CDS, SESSION KEYS (Kses3,4) SHARED
S721
MUTUAL AUTHENTI-CATION, SESSION KEYS (Kses3,4) SHARED
S712
ATTACH MAC (MAC4) TO SELECTED Right AND SPECS INFORMATION WITH Kses3 AND TRANSMIT
RECEIVE Right AND SPECS INFORMATION AND MAC4
S722
S723
IS MAC4 CORRECT?
NO
YES
END IN ERROR
S724
VERIFY SIGNATURE SIGrss OF Right WITH CORRESPONDING PUBLIC KEY PUBrss
S725
IS SIGrss CORRECT?
NO
YES
S726
IDright CONFIRMED TO BE WITHIN VALIDITY PERIOD (VID CONFIRMED)?
NO
YES
END IN ERROR
S701
MUTUAL AUTHENTI-CATION
S713
RECEIVE CONTENTS AND MAC5, MUTUAL AUTHENTICATION WITH RHD DURING RECEPTION TO CONFIRM EXISTENCE
SEARCH CONTENTS CORRESPONDING TO Right AND SPECS INFORMATION FROM CONTENTS DATABASE
S727
S714
IS MAC5 CORRECT?
NO
YES
END IN ERROR
ENCRYPT Encryption Key WITHIN Header WITH Kses4
S728
S715
PREPARE STREAMING PLAYBACK BASED ON INFORMATION IN Header
ATTACH MAC (MAC5) ONLY TO Header WITH Kese3 AND TRANSMIT
S729
S716
TRANSMIT DATA TRANSMISSION REQUEST
RECEIVE DATA TRANSMISSION REQUEST
S730
S702
S717
MUTUAL AUTHENTI-CATION
PLAY DATA WHILE DECRYPTING WITH Kses4
ENCRYPT STREAMING DATA WITH Kses4 AND TRANSMIT
S731
END
END
END

FIG. 20

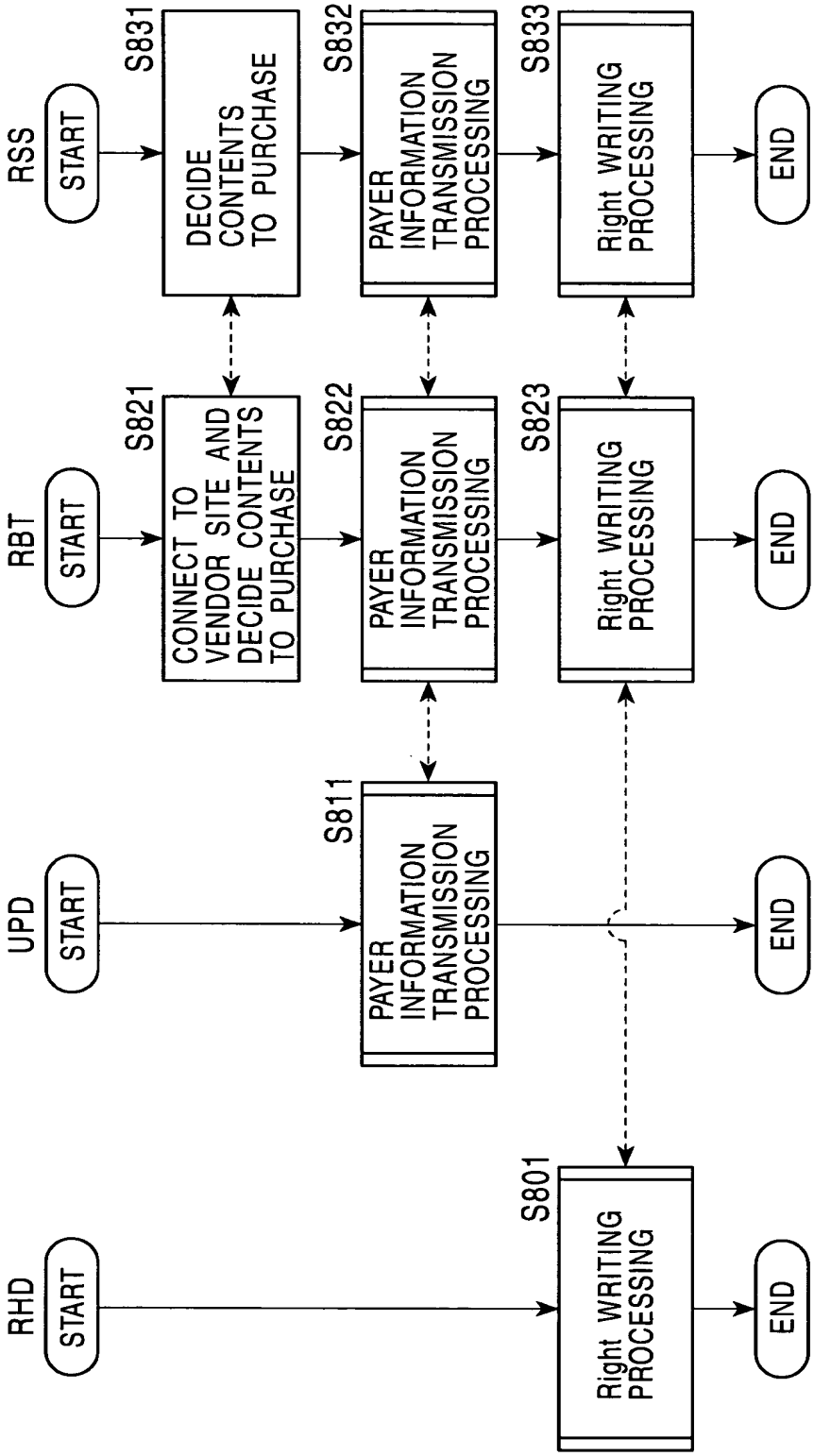

RSS
START
S831
DECIDE CONTENTS TO PURCHASE
S832
PAYER INFORMATION TRANSMISSION PROCESSING
S833
Right WRITING PROCESSING
END
RBT
START
S821
CONNECT TO VENDOR SITE AND DECIDE CONTENTS TO PURCHASE
S822
PAYER INFORMATION TRANSMISSION PROCESSING
S823
Right WRITING PROCESSING
END
UPD
START
S811
PAYER INFORMATION TRANSMISSION PROCESSING
END
RHD
START
S801
Right WRITING PROCESSING
END

FIG. 21

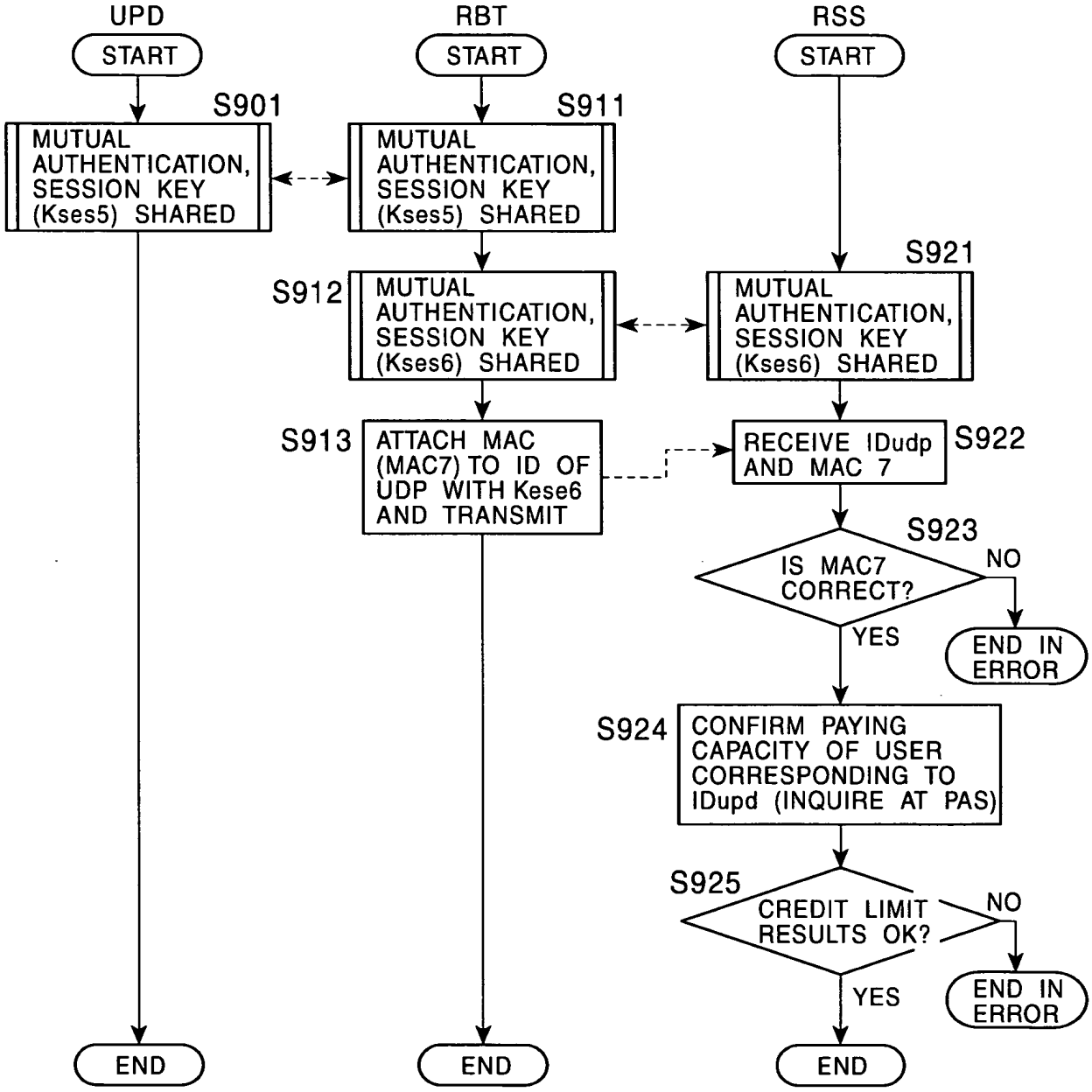
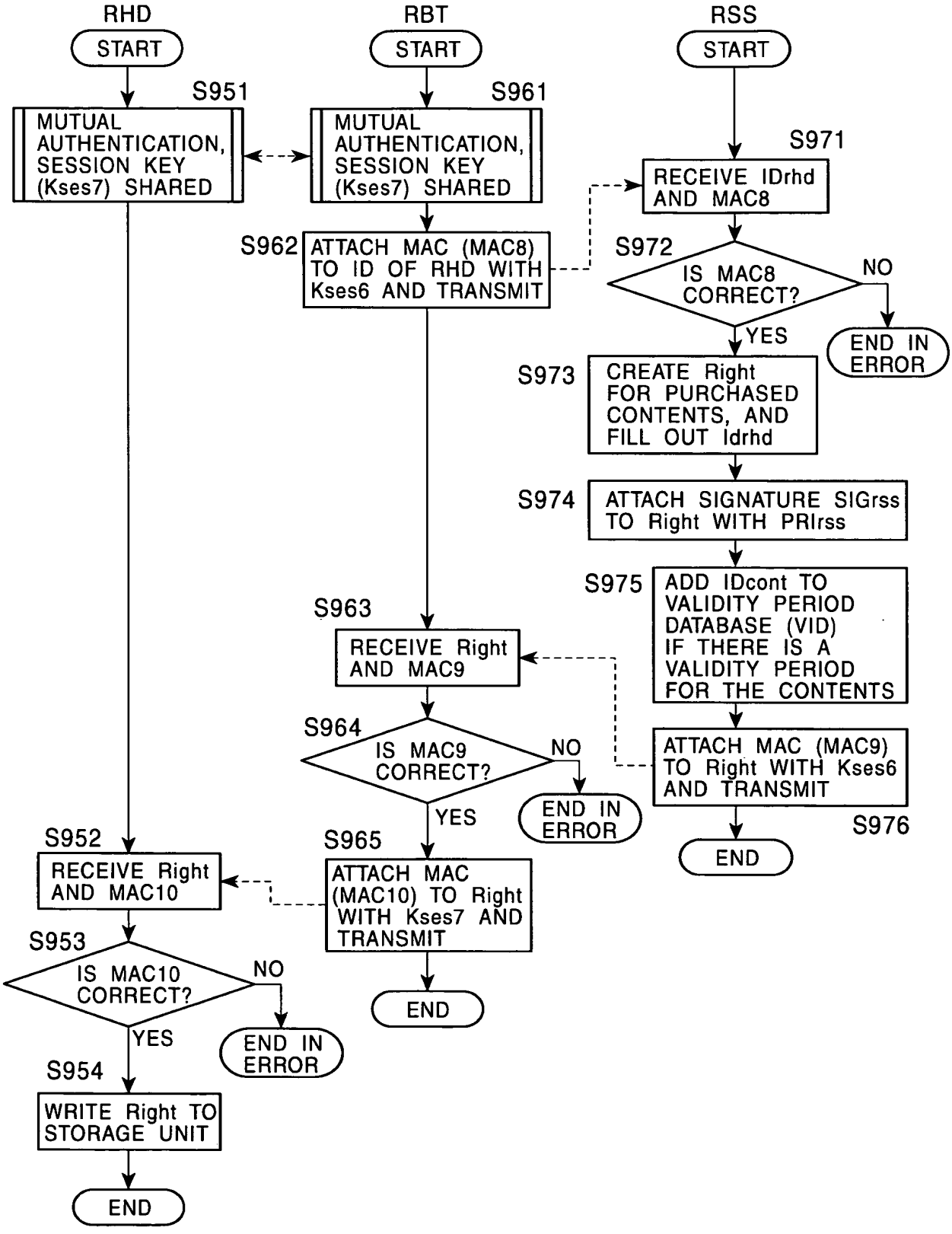

UPD
START
S901
MUTUAL AUTHENTICATION, SESSION KEY (Kses5) SHARED
END
RBT
START
S911
MUTUAL AUTHENTICATION, SESSION KEY (Kses5) SHARED
S912
MUTUAL AUTHENTICATION, SESSION KEY (Kses6) SHARED
S913
ATTACH MAC (MAC7) TO ID OF UDP WITH Kese6 AND TRANSMIT
END
RSS
START
S921
MUTUAL AUTHENTICATION, SESSION KEY (Kses6) SHARED
RECEIVE IDudp AND MAC 7
S922
S923
IS MAC7 CORRECT?
NO
END IN ERROR
YES
S924
CONFIRM PAYING CAPACITY OF USER CORRESPONDING TO IDupd (INQUIRE AT PAS)
S925
CREDIT LIMIT RESULTS OK?
NO
END IN ERROR
YES
END

FIG. 22


RHD
START
S951
MUTUAL AUTHENTICATION, SESSION KEY (Kses7) SHARED
S952
RECEIVE Right AND MAC10
S953
IS MAC10 CORRECT?
NO
END IN ERROR
YES
S954
WRITE Right TO STORAGE UNIT
END
RBT
START
S961
MUTUAL AUTHENTICATION, SESSION KEY (Kses7) SHARED
S962
ATTACH MAC (MAC8) TO ID OF RHD WITH Kses6 AND TRANSMIT
S963
RECEIVE Right AND MAC9
S964
IS MAC9 CORRECT?
NO
END IN ERROR
YES
S965
ATTACH MAC (MAC10) TO Right WITH Kses7 AND TRANSMIT
END
RSS
START
S971
RECEIVE IDrhd AND MAC8
S972
IS MAC8 CORRECT?
NO
END IN ERROR
YES
S973
CREATE Right FOR PURCHASED CONTENTS, AND FILL OUT Idrhd
S974
ATTACH SIGNATURE SIGrss TO Right WITH PRIrss
S975
ADD IDcont TO VALIDITY PERIOD DATABASE (VID) IF THERE IS A VALIDITY PERIOD FOR THE CONTENTS
ATTACH MAC (MAC9) TO Right WITH Kses6 AND TRANSMIT
S976
END